

TECHNIQUE T845: PROGRAM UPLOAD

CyOTE Use Case(s)	MITRE ATT&CK for ICS® Tactic
Alarm Logs, HMI	Collection
Data Sources	
Potential Data Source(s)	Alarm Logs, Application Logs, Device Logs, Event Records, Firewall Logs, Hashes of Control Logic Payload, Host Logs, Log-In Activity, Operating System Logs, Packet Captures, VPN Logs
Historical Attacks	Triton Attack at Petro Rabigh ¹

TECHNIQUE DETECTION

The Program Upload technique² (Figure 1) may be detected via analyzing operational technology (OT) traffic and via deep packet inspection to identify potential indicators arising from an attempt to upload information. Device logs may also be leveraged as a data source to trigger network traffic capture and assist network capture analysis.

To augment commercial sensor gaps, the CyOTE program has developed capabilities such as Proof of Concept tools³ and Recipes⁴ for asset owners and operators (AOO) to identify indicators of attack for techniques like Program Upload within their operational technology (OT) networks. Referencing CyOTE Case Studies⁵ of known attacks, AOOs in both small and large organizations can utilize CyOTE's Use Case analyses to tie operational anomalies and observables to cyber-attack campaigns resulting in ever-decreasing impacts.

PERCEPTION: OBSERVABLES FROM HISTORICAL ATTACKS

The Program Upload technique was used in the Triton attack at Petro Rabigh in 2017.⁶ In this attack, the following observables were identified:

- Increased internet traffic

¹ MITRE, *Software: Triton, TRISIS, HatMan*, <https://collaborate.mitre.org/attackics/index.php/Software/S0013>

² MITRE ATT&CK for ICS, T845: Program Upload, <https://collaborate.mitre.org/attackics/index.php/Technique/T0845>

³ A Proof of Concept tool is a representative implementation of a set of steps and methods for identifying techniques. A Proof of Concept tool is defined as a script(code) or using capabilities of existing tools (e.g., Splunk, Gravwell), to demonstrate the capability to identify adversarial activity for a selected technique. A Proof of Concept tool is not ready for implementation in an AOO's environment as its major focus is to a specific instance (device, vendor, protocol, scenario) in order to prove a concept.

⁴ A Recipe is a set of steps and methods for identifying techniques. Recipes can be used to develop a Proof of Concept or operational tool in an AOO's OT environment.

⁵ Visit <https://inl.gov/cyote/> for all CyOTE Case Studies.

⁶ <https://www.eenews.net/stories/1060123327>

- Application logs indicating programs are being uploaded to other devices

Disclaimer: Past occurrences are not guaranteed to occur in future attacks.

COMPREHENSION

In the Triton attack at Petro Rabigh, the adversary first gained access through an engineering workstation to map the network; once they gained control of the workstation, they transferred payloads to the devices, the process for which includes performing a program upload. They then moved through the network and modified operating modes and device logic to issue malicious command messages that shut down part of the plant.⁷ By understanding the nature and possible origins of this attack, as well as how the adversary used the Program Upload technique to execute the attack, an AOO can better comprehend how this technique is used with others and enhance their capabilities to detect attack campaigns using this technique and decrease an attack's impacts.

CURRENT CAPABILITY

The CyOTE Recipe outlines a process to analyze operational technology (OT) network traffic and use deep packet inspection to identify potential indicators arising from an attempt to upload information.

POTENTIAL ENHANCEMENTS

The process can be enhanced by leveraging device logs to trigger network traffic capture and assist network capture analysis.

ASSET OWNER DEPLOYMENT GUIDANCE

The CyOTE Recipe can be leveraged to develop an operational tool. This tool should be deployed by a network team, in conjunction with cyber defenders and operators, to a host capable of processing the desired amount of traffic in an acceptable time frame. This host will either need access to a span port for live traffic or stored Packet Capture (PCAP) files awaiting to be processed. The operational tool can be configured and populated with supporting information regarding approved hosts.

AOOs can refer to the CyOTE Technique Detection Capabilities report (visit <https://inl.gov/cyote/>) for more information on the background and approach of CyOTE's technique detection capabilities.

AOOs can also refer to the [CyOTE methodology](#) for more information on CyOTE's approach to identifying anomalies in an OT environment, which, when perceived, initiates investigation and analysis to comprehend the anomaly.

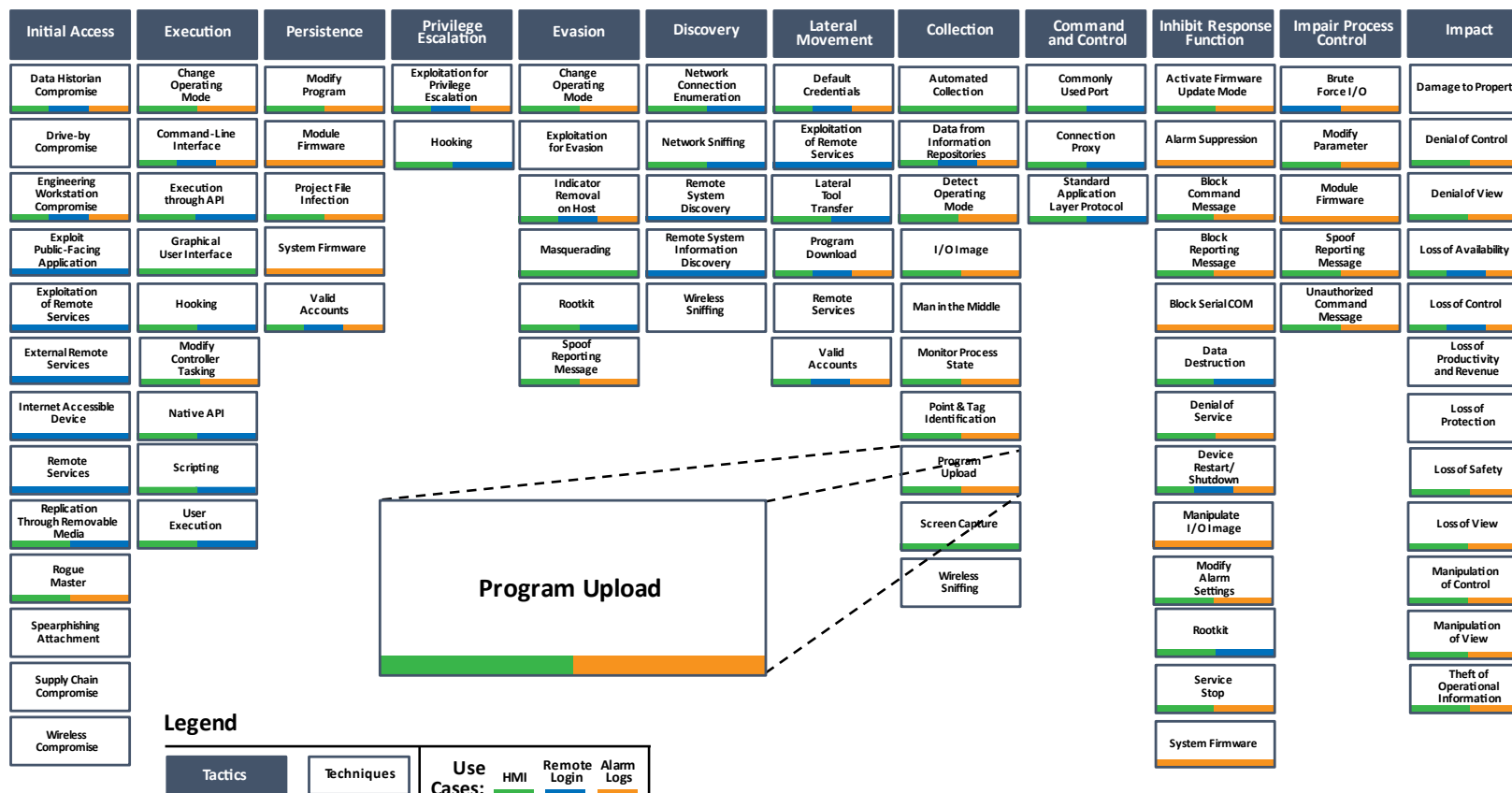
⁷ CyOTE Case Study: Triton in Petro Rabigh. <https://inl.gov/wp-content/uploads/2021/09/Triton-CyOTE-Case-Study.pdf>

Click for More Information

[CyOTE Program](#) || [Fact Sheet](#) || CyOTE.Program@hq.doe.gov

DOE Senior Technical Advisor

Edward Rhyne || Edward.Rhyne@hq.doe.gov || 202-586-3557



MITRE ATT&CK for ICS Matrix (April 2021)

Figure 1: ICS ATT&CK Framework⁸ – Program Upload Technique

⁸ © 2021 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.
https://collaborate.mitre.org/attackics/index.php/Main_Page.